[19]中华人民共和国国家知识产权局

[51]Int.Cl[6]
G06F 17/60

[12]发明专利申请公开说明书

[21]申请号 97192329.9

[43]公开日 1999年3月17日

[11]公开号 CN 1211330A

[22]申请日 97.2.19 [21]申请号 97192329.9

[30]优先权
[32]96.2.21 [33]JP [31]70834/96

[86]国际申请 PCT/JP97/00434 97.2.19

[87]国际公布 WO97/31321 日 97.8.28

[85]进入国家阶段日期 98.8.17

[71]申请人 卡式通讯系统股份有限公司
地址 日本东京

[72]发明人 马场芳美

[74]专利代理机构 上海专利商标事务所
代理人 孙敬国

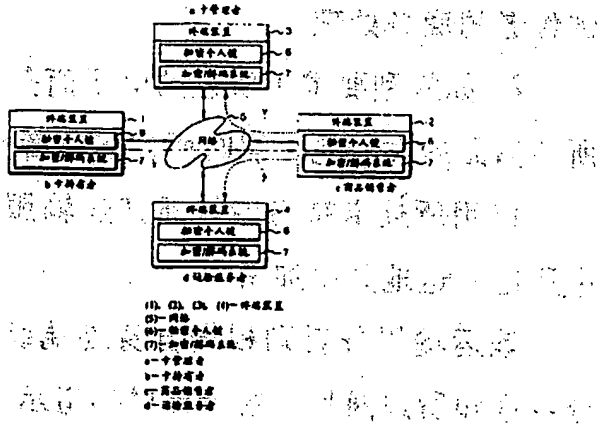
权利要求书2页 说明书10页 附图页数3页

[54]发明名称 电子商务处理系统

[57]摘要

本发明在利用货款支付用卡联机通信的电子商务处理系统中，提供一种消除假冒商品销售者危险性、确保商务处理安全性且简易通用的电子商务处理系统。

持有卡的卡持有者欲从商品销售者购买商品时，通过卡持有者的终端装置1分别用只与当事者间有效的公用密码键对用于这种购买的定购数据中与商品销售者、卡管理者及运输服务者各当事者有关的部分数据加密，并经由商品销售者终端装置2将这些加密数据通信发送给各当事者的终端装置2～3。各当事者用与卡持有者公用的密码键对与自己有关的部分数据解码，进行所需的商务处理。



权 利 要 求 书

1. 一种电子商务处理系统，其特征在于，是一种至少将商品销售者、使用货款支付用卡从所述商品销售者购入商品的卡持有者、和对利用该卡完成货款支付进行管理的卡管理者作为当事者，通过包含各当事者具有的终端装置在内的网络中联机通信进行商务处理的系统，

当所述卡持有者使用所述卡从所述商品销售者购入商品时，该卡持有者通过本身终端装置用仅分别与各当事者间有效的公用密码键对购入所述商品用定购数据中除该卡持有者外的与各当事者相关的部分加密后，将包括这些加密后的数据一起构成的加密定购数据从该卡持有者终端装置经由所述商品销售者终端装置通信发送到除该卡持有者外的各当事者，

接收到该加密定购数据的各当事者通过各自终端装置用与所述卡持有者公用的所述公用密码键对所述加密定购数据中仅涉及本身的部分数据进行解码，

在进行这种解码的当事者中，所述卡管理者根据自身终端装置解码后的部分数据，进行包括向所述商品销售者提供对所述卡持有者认证的处理在内的涉及卡管理者的商务处理，

所述商品销售者根据自身终端装置解码后的部分数据和所述卡管理者已提供的对所述卡持有者的认证，进行包括为发送所述商品的处理在内的涉及该商品销售者的商务处理。

2. 如权利要求 1 所述的电子商务处理系统，其特征在于，所述定购数据包含所述商品的发送地，同时所述当事者包括发送所述商品的运输服务者，

仅用所述卡持有者及所述运输服务者间的所述公用密码键对所述定购数据中所述发送地数据加密，

该运输服务者则根据自身终端装置解码后的包含所述发送地数据的所述部分数据和所述商品销售者提供的指示进行所述商品的发送处理。

3. 如权利要求 1 所述的电子商务处理系统，其特征在于，所述定购数据包含所述卡的号码及有效期，该号码及有效期的数据仅用所述卡持有者及卡管理者间公用的所述公用密码键加密。

4. 如权利要求 1 所述的电子商务处理系统，其特征在于，所述卡持有者与该

持有者以外各当事者固有且公开的标识符作用于该卡持有者预先备有的该卡持有者固有的秘密个人键而生成，在该卡持有者以外的各当事者一侧，是使所述卡持有者固有且公开的标识符作用于该当事者预先备有的该当事者固有的秘密个人键而生成.

5. 如权利要求 1 所述的电子商务处理系统，其特征在于，在进行所述加密定购数据通信前，所述各当事者可预先与该加密定购数据的通信对方相互通信，对该通信对方的当事者进行确认.

说 明 书

电子商务处理系统

技术领域

本发明涉及应用国际互联网(internet)、个人计算机通信等联机通信，进行商务处理的电子商务处理系统，具体涉及使用信用卡、记帐卡等货款支付用卡的电子商务处理系统.

背景技术

近年来，随着国际互联网、个人计算机通信等的普及，这些网络用户通常已经借助国际互联网上的电子邮购或个人计算机通信向商店等商品销售者通过联机通信以定购所需商品，进行该商品的购买.

在这种商务处理中，想要购入商品的客户预先持有信用卡、记帐卡等货款支付用卡，在购入商品时，从该卡持有者的终端装置经网络向商品销售者通信发送该购买者即卡持有人的姓名、地址、电话号码和要购买商品种类、数量等数据，以及该卡持有人的卡的号码及有效期等数据. 然后，商品销售者根据在自己的终端装置接收到的上述数据从卡管理者(发卡公司)对卡持有者进行认证，并进行商品发送手续(包括向运输服务者委托商品发送)和向发卡公司请求支付货款等处理. 而发卡公司进行如下处理，即根据商品销售者提供的卡持有者姓名、住所、电话号码、卡号码及有效期等将为商品销售者进行卡持有者的认证，再根据商品销售者提供的商品货款等数据从卡持有者户头中扣除商品货款(商品货款结帐)等.

在上述电子商务处理系统中，已往已经指出存在侵入(hacking 窃取通信数据)、击破(craking，篡改通信数据)、或假冒卡持有者、商品服务器(商品销售者终端)获取者网关(acquirer gateway，卡管理者终端)等的危险性.

此时，如对于假冒卡持有者，可借助卡管理者保管的卡号码等数据库，在一定程度上加以防止. 另外，通常对每个卡持有者的卡的支付金额，设定其上限，故假冒卡持有者造成的损失不会有太大的金额.

集多个卡号码，有效期等卡的信息，因盗用这些卡信息，故会产生比上述大得多的损失.

作为解决上述问题的对策，已往采用卡持有者的识别号(ID 号)和口令、或与它们相当的数据进行通信，或通常构筑封闭式用户组(closed user group)，使得所述识别号和通行字即使被盗用，也不会对利用该卡已进行的商务处理带来影响.但是，采用上述系统要想解决上述问题是困难的.

另外，虽然人们在不断地提出用 DES 等流式公用键密码对通信数据加密和用 RSA 密码等公开键密码进行认证等针对上述各个问题的对策方案，但实际上仍未构筑成简单通用的电子商务处理系统.

本发明鉴于上述背景技术情况，其目的在于在利用货款支付用卡联机通信的电子商务处理系统中，提供一种能消除假冒商品销售者等带来危害性的确保商务处理安全性且简易通用的电子商务处理系统.

本发明的揭示

为完成上述发明目的，本发明的电子商务处理系统是一种至少将商品销售者、使用货款支付用卡从所述商品销售者购入商品的卡持有者和对利用该卡完成货款支付进行管理的卡管理者作为当事者，通过包含各当事者具有的终端装置在内的网络中联机通信进行商务处理的系统，其特征在于，当所述卡持有者使用所述卡从所述商品销售者购入商品时，该卡持有者通过本身终端装置用仅分别与各当事者间有效的公用密码键对购入所述商品用定购数据中除该卡持有者外的与各当事者相关的部分加密后，将包括这些加密后的数据一起构成的加密定购数据从该卡持有者终端装置经由所述商品销售者终端装置通信发送到除该卡持有者外的各当事者，接收到该加密定购数据的各当事者通过各自终端装置用与所述卡持有者公用的所述公用密码键对所述加密定购数据中仅涉及本身的部分数据进行解码，在进行这种解码的当事者中，所述卡管理者根据自身终端装置解码后的部分数据，进行包括向所述商品销售者提供对所述卡持有者认证的处理在内的涉及卡管理者的商务处理，所述商品销售者根据自身终端装置解码后的部分数据和所述卡管理者已提供的对所述卡持有者的认证，进行包括为发送所述商品的处理在内的涉及该商品销售者的商务处理.

者用仅在各当事者间有效的公用密码键对所述定购数据中涉及所述商品销售者和卡管理者等除该卡持有者外的各当事者的部分数据进行加密，在此基础上，从该卡持有者终端装置经由商品销售者终端装置将这些加密后数据解码构成的加密定购数据通信发送给包含该商品销售者在内的各当事者．这样一来，通过对定购数据加密，故能保住其机密性．

此外，收到该加密定购数据的商品销售者、卡管理者等各当事者，用与所述卡保持者间的公用密码键从该加密定购数据中解码出与该当事者有关的部分数据．此时，对于仅涉及及其它当事者的部分数据而言，各当事者因没有用于对其解码的公用密码键，故不能获知该部分数据解码后的内容，换言之，所述当事者仅能在相关范围内知道所述定购数据的内容．因此，当事者不能盗用与其无关的部分数据．因而，所述当事者中，卡管理者根据解码后部分数据进行包含向所述商品销售者提供对所述卡持有者认证的处理在内的涉及该卡管理者的商务处理，所述商品销售者根据自身终端装置解码后的部分数据和所述卡管理者提供的对所述卡持有者的认证，进行包含向所述卡持有者递送所述商品的处理在内的涉及该商品销售者的商务处理．由此，可进行电子商务处理．

因此，按照本发明，对定购数据加密后进行通信，故能确保其机密，同时所述卡持有者外的各当事者只能获知所述定购数据中所需最低限度的数据．为此，假设即使有第三者假冒商品销售者，该假冒的商品销售者也不能获取如卡号码或有效期等仅与卡管理者有关的信息，从而假冒商品销售者不能获得实际效果．由此，按照本发明，能消除假冒商品销售者等的危险性，并能确保商务处理的安全性．另外，在所述卡持有者终端装置中生成的加密定购数据由于经由商品销售者分配给各当事者，故卡持有者购买商品时，实质上只要将所述加密定购数据仅通信发送给商品销售者即可，从而能实现简单的电子商务处理系统．

在上述本发明电子商务处理系统中，有时所述定购数据也包含所述商品的发送地(它不限于所述卡持有者的地址)，另外，作为所述当事者有时也还包括发送商品的运输服务者．

然而此时，最好仅用所述卡持有者及所述运输服务者间的所述公用密码键对所述定购数据中所述发送地数据加密，该运输服务者则根据自身终端装置解码后的包含所述发送地数据的所述部分数据和所述商品销售者提供的指示进行所述

务者知道，从保密性的观点来看更为理想.

在本发明中，所述定购数据包含所述卡的号码及有效期，该号码及有效期的数据仅用所述卡持有者及卡管理者间公用的所述公用密码键加密．由此，使用所述货款支付用卡进行商务处理时，在实际结帐中最为重要的卡号码及有效期只能由必须知道该数据的所述卡管理者对所述加密定购数据解码后获知；反而言之，除该卡管理者及卡持有者外的当事者不能获得卡号码及有效期的数据．因此，能有效确保所述电子商务处理系统的安全性，同时能有效地防止在该商务处理中危险性最高的假冒商品销售者.

在以上所述本发明中，所述公用密码键，虽可用预先确定的其它办法在所述卡持有者与各当事者间进行均等分配，但所述卡持有者与该卡持有者以外的各当事者间的所述公用码键，在所述卡持有者一侧，最好是使该卡持有者以外各当事者固有且公开的标识符作用于该卡持有间预先备有的该卡持有者固有的秘密个人键而生成；在该卡持有者以外的各当事者一侧，最好使所述卡持有者固有且公开的标识符作用于该当事者预先备有的该当事者固有的秘密个人键而生成．这里，所述标识符可以是各当事者姓名，名称，住所，网络上的邮址，区域名或它们的组合等各当事者固定使用且公开的信息.

这样一来，包括卡持有者的各当事者采用使应共有公用密码键的对方的标识符作用于自的所述秘密个人键来生成公用密码键的方式，各当事者只是将对方的标识符输入自己的秘密个人键而不事前确定或分配公用密码键，能够生成为所述商务处理所需的公用密码键．因此，本发明的电子商务处理系统可极其简单，且通用性强．而且公用密码键本身无需事先配置；故能确保通信数据的机密性，并能提高电子商务处理系统的安全性.

关于上述公用密码键的生成方式，例如在 Rolf Blom 的论文“NON - PUBLIC KEY DISTRIBUTION/Advances in Cryptology: Proceedings of CRYPTO '82/Plenum Press 1983, pp.231-236”，同样是 Rolf Blom 的论文“An Optimal Class of Symmetric Key Generation Systems/ Advances in Cryptology: EUROCRYPT '84/Springer LNCS 209,1985,pp. 335-338”或特公平 5－48980 号公报等中有揭示，这里省略其详细说明.

本发明在进行上述加密定购数据通信前，上述各当事者最好预先与该加密定

先进行电子商务处理有关当事者的确认，能事先防止假冒商品销售者或卡管理者等带来的危害，从而进一步提高电子商务处理系统的安全性.

附图概述

图1为本发明一实施形态电子商务处理系统的系统结构图，图2为表示图1系统中卡持有者侧数据处理的说明图，图3为表示图1系统中除卡持有者外的当事者侧数据处理的说明图.

实施本发明的最佳形态

参照图1及图2说明本发明一实施形态.

参看图1，本实施形态的电子商务处理系统中，持有信用卡(credit cart)、记帐卡(debit card)等货款支付用卡(未图示)的卡持有者的终端装置1，商品销售者终端装置2，对利用该卡完成货款支付进行管理的卡管理者(发卡公司)的终端装置3，担当商品销售者经营商品的发送业务的运输服务者的终端装置4，经国际互联网(internet)、个人计算机通信网等网络5相互连接，能够进行通信. 这些卡持有者，商品销售者，卡管理者及运输服务者成为下文叙述的电子商务处理的当事者.

各当事者终端装置1～4由个人计算机等计算机装置构成. 这些终端装置1～4包含用于在任何当事者间生成密码通信用公用密码键的公用密码键生成用系统的秘密个人键6，和用于这种公用密码键产生的通信数据加密/解码的加密/解码系统7，它们由软件或硬件构成，由未图示的发行密码键等中心事先将这些系统6、7分配给当事者.

这里，上述秘密个人键6如上述Rolf Blom的论文或特公平5－48980号公报等中所见，为各当事者所固有，通过将通信对方的姓名、位所等各当事者所固有且公开的标识符输入各终端装置1～4，生成与其通信的对方公用的公用密码键.

上述加密/解码系统7采用公知的DES(Data Encryption Standard: 数据加密标准)，借助所述公用密码键对通信数据加密(通信数据发送侧)，或对该加密后的通信数据解码(通信数据接收侧).

理.

首先，在本实施形态的系统中，各当事者通过网际互联网或个人计算机通信等，可借助各终端装置 1 - 4 随时与要进行下述加密定购数据通信的对方相互进行通信，由此，可事先确认作为应进行下述加密定购数据通信的当事者彼此的对方是否正确(通信对方的认证).

卡持有者事先通过自身终端装置 1 与商品销售者终端装置 2 的通信(参看商品销售者的主页面(home page)等)，或通过 CD - ROM 等记录媒体或杂志等参看商品销售者的商品目录，来获取商品销售者的商品信息.

当卡持有者要购买商品销售者的商品时，将其想法从卡持有者通知商品销售者，该商品销售者发送定购单格式的数据. 该定购单格式数据也可由卡持有者自己事先从 CD - ROM 获取.

接着，卡持有者按照取得的定购单格式通过自身终端装置 1 输入定购数据以便用自己的卡购买想要的商品. 此时，作为输入的定购数据如图 2 所示有：卡持有者的姓名，住所，电话号码，传真号，卡持有者具有的卡号码及有效期，欲购买的商品的品名，数量，商品号，购买金额，货款支付方式(分期付款，一次性付款等)，商品的发送地(包括收件人姓名，住所等)等.

该定购数据当然不限于上述数据，只要包含卡持有者使用自己卡购买商品时作为该商务处理的当事者的商品销售者、卡管理者及运输服务者执行与该商品处理有关的各自处理(商品销售者确定定购者或定购内容，卡管理者对卡持有者进行认证及对货款进行结算，运输服务者发送商品等)所需的信息.

在作成上述定购数据后，卡持有者再通过自身的终端装置 1 从该定购数据中分别提取与商品销售者、卡管理者及运输服务者等各当事者有关部分的数据(这些预先加以确定)，并加以复制. 参照图 2，如涉及商品销售者，从上述定购数据中复制卡持有者姓名，住所，电话号码，传真号，欲购商品的品名，数量，商品号，购买金额，货款的支付方式等用于确定定购者或定单内容的数据，与卡管理者有关的，则复制卡持有者姓名，住所，电话号码，传真号，卡持有者所具有的卡号及有效期，欲购商品的商品号，购买金额，货款支付方式等用于认证卡持有者或结算货款的数据. 涉及运输服务者的，则复制卡持有者姓名，电话号码，传真号，发送地等为发送商品所必需的数据.

向卡持有者发送所述定购单格式数据时，预先提供给该卡持有者．然后，卡持有者按照进行上述处理的程序或按照所给的软件进行．各当事者的每部分数据不限定于上述形态，例如所述传真号数据有时对所有当事者而言都不需要，另外，按照各国法律或习惯，卡管理者可不需要商品号，或商品销售者需要商品发送地．

进而卡持有者将商品销售者、卡管理者及运输服务者各当事者的标识符分别输入其终端装置 1 中的所述秘密个人键 6，分别生成与这些各当事者间密码通信用的所述公用密码键．此时，运输服务者由商品销售者确定，该运输服务者的标识符或卡持有者识别它所需信息(运输服务者的名称等)在如商品销售者将所述定购单格式数据发送给卡持有者时等事先供给该卡持有者．商品销售者及卡管理者由卡持有者本身确定，故该卡持有者已经知道商品销售者及卡管理者的标识符．

这样一来，从所述定购数据复制与商品销售者、卡管理者及运输服务者等各当事者有关的部分数据及生成与这些各当事者间的公用密码键后，卡持有者通过自身终端装置 1 的所述加密/解码系统 7，如图 2 所示，用对应于各当事者的公用密码键对与各当事者有关部分数据加密，接着，将该加密后的各部分数据一起构成的加密定购数据与卡持有者的标识符作为一组通信数据从本身终端装置 1 经网络 5 发送给商品销售者的终端装置 2(参看图 1 中虚线箭头 X)．此时，与加密定购数据一起发送的卡持有者标识符未经加密．另外，也可与加密定购数据一起发送由商品销售者等各当事者能指定卡持有者标识符的信息(仅取卡持有者的姓名、住所等)来代替卡持有者的标识符．

此时，上述通信数据主要部分的加密定购数据，由于加了密，故不是当事者的第三者不能对其解读，能确保该通信数据的机密性．

此外，在终端装置 2 接收到上述通信数据(加密定购数据及卡持有者标识符)的商品销售者将包含在该通信数据中的卡持有者标识符输入自身终端装置 2 的秘密个人键 6，生成与卡持有者共用的公用密码键．参看图 3，商品销售者用所生成的公用密码键通过自身终端装置 2 的所述加密/解码系统 7 对所述加密定购数据中涉及本身的部分数据进行解码．由此，正式获取所述定购数据中持卡者的姓名，住所，电话号码，传真号，欲购商品的品名，数量，商品号，购买金额，货款支付方式等商品销售者所必需的数据．

此时，涉及商品销售者以外的当事者(卡管理者及运输服务者)的部分数据，

者不能对这些部分数据解码，因此，不能获知如涉及卡管理者的卡号码或有效期或涉及运输服务者的发送地数据的内容.

进而，商品销售者从自身终端装置2经网络5向卡管理者终端装置3发送所述加密定购数据及卡持有者的标识符(参见图1中虚线箭头Y)。此时，虽可将商品销售者接收到的所有数据发送给卡管理者，但也可向卡管理者发送加密定购数据中仅与卡管理者有关的部分数据及卡持有者的标识符.

这样一来，用自身终端装置3从商品销售者终端装置2接收到加密定购数据及卡持有者标识符的卡管理者，与商品销售者情况一样，在将卡持有者标识符输入自身终端装置3的秘密个人键6生成与卡持有者公用的公用密码键后，如图3所示，用该公用密码键通过自身终端装置3中所述加密/解码系统7对所述加密定购数据中与自身有关的部分数据解码。由此，从所述定购数据中正式获取卡持有者的性名，住所，电话号码，传真号，卡持有者具有的卡号码及有效期，欲购商品的商品号，购买金额，货款支付方式等卡管理者所需数据。此时，卡管理者与商品销售者情况一样，不能获知所述加密定购数据中与自身无关的如仅与运输服务者有关的商品发送地等数据.

此后，获取上述数据的卡管理者，根据卡持有者的姓名，电话号码，卡号码及有效期等数据，对卡持有者进行认证(卡持有者是不是正当的卡用户)，并将该认证结果通知商品销售者。若卡持有者为正当卡用户，则按购买金额、货款支付方式等数据进行处理，以便从卡持有者的启头中扣除货款.

若该认证结果正确，则接收到卡管理者来的该认证结果通知的商品销售者从自身终端装置2经网络5向运输服务者终端装置4发送所述加密定购数据及卡持有者标识符(参看图1中虚线箭头Z)，同时根据该商品销售者获得的部分数据向运输服务者委托商品发送，再根据需要安排商品进货等。此时，也可将加密定购数数据中仅与运输服务者有关的部分数据与卡持有者标识符一起发送给运输服务者.

然后，与商品销售者及卡管理者的情况一样，从商品销售者接收到加密定购数据及卡持有者标识符的运输服务者，在将卡持有者标识符输入自身终端装置4的秘密个人键6生成与卡持有者公用的公用密码键后，如图3所示，用该公用密码键通过自身终端装置4中所述加密/解码系统7对所述加密定购数据中与自身有

传真号，发送地等运输服务业者所必需的数据。此时，运输服务者与商品销售者或卡管理者情形一样，不能获知所述加密定购数据中与自身有关数据以外的如卡号码及有效期等数据。

获取上述发送地等数据的运输服务者根据该数据和商品销售者的指示，进行商品发送。

在如上构成的本实施形态的电子商务处理系统中，分别用与各个当事者间各个不同的公用密码键对卡持有者作成的定购数据中与各当事者(商品销售者、卡管理者及运输服务者)有关的数据进行加密，并经通信将这些加密后的部分数据分配给各当事者，故能确保定购数据的机密性。同时，各当事者利用与卡持有者间的公用密码键可自由获取定购数据中所需数据，另一方面反过来说也只能获知必要数据。因此，如商品销售者或运输服务者则不能获知用卡进行商务处理上最重要的卡号或有效期。为此，假设即使第三者假冒商品销售者或运输服务者，由于不能获得卡号码或有效期等重要信息，因而也不会得逞，从而能防止假冒商品销售者或运输服务者。

包括卡持有者在内的各当事者事先与要进行所述加密定购数据通信的对方进行通信，确认对方当事者，故不仅能防止假冒商品销售者或运输服务者，还能防止假冒卡管理者。

本申请的发明人用本实施形态的电子商务处理系统进行的试验证实，在种种假冒等侵入系统的情况下，能完全抵制这类侵入。

在该实施形态中，只用运输服务者与卡持有者间的公用密码键对商品发送地加密，故商品销售者或卡管理者不能获知该数据，因此，卡持有者在将所购商品赠予别人等情况下能加以保密。

卡持有者欲购商品时，所述加密定购数据经由商品销售者终端装置2分送给该商品销售者外的卡管理者或运输服务者，故卡持有者只要将加密定购数据发送给商品销售者终端装置2就可以，能方便地购买商品。

在本实施形态中，卡持有者对与商品销售者、卡管理者及运输服务者有关的部分数据加密，而且各当事者只要将所需当事者的标识符输入设于自身终端装置(图1-4)中的秘密个人键，就能生成商品销售者、卡管理者及运输服务者将自己部分数据进行解码用的公用密码键，故每当进行商务处理时，没有必要决定当事者

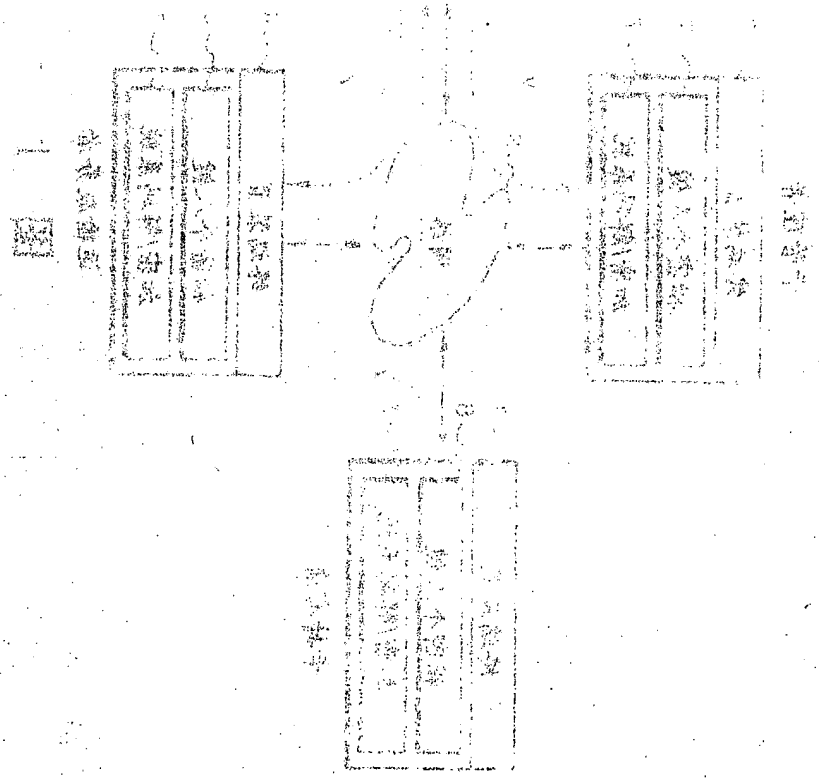
因此，本实施形态的电子商务处理系统可作为一种安全、简单、具有通用性的系统.

在以上说明的本实施形态中，所示系统包含运输服务者作为电子商务处理当事者，但也可构成不包含该运输服务者的系统，或构成包含国际互联网供应商(internet provider)等网关(gateway)管理者或键认证局等作为当事者的系统.

在本实施形态中，所示系统由各当事者将所需当事者的标识符输入设于自身终端装置 1 - 4 的秘密个人键来生成公用密码键，但也可以用其它办法在当事者间确定公用密码键或从中心分配公用密码键.

工业上的可应用性

本发明能适用于在国际互联网、个人计算机通信网等网络上通过用个人计算机等终端装置联机通信使用信用卡或记帐卡等货款支付用卡进行商务处理的系统.



说 明 书 附 图

图 1

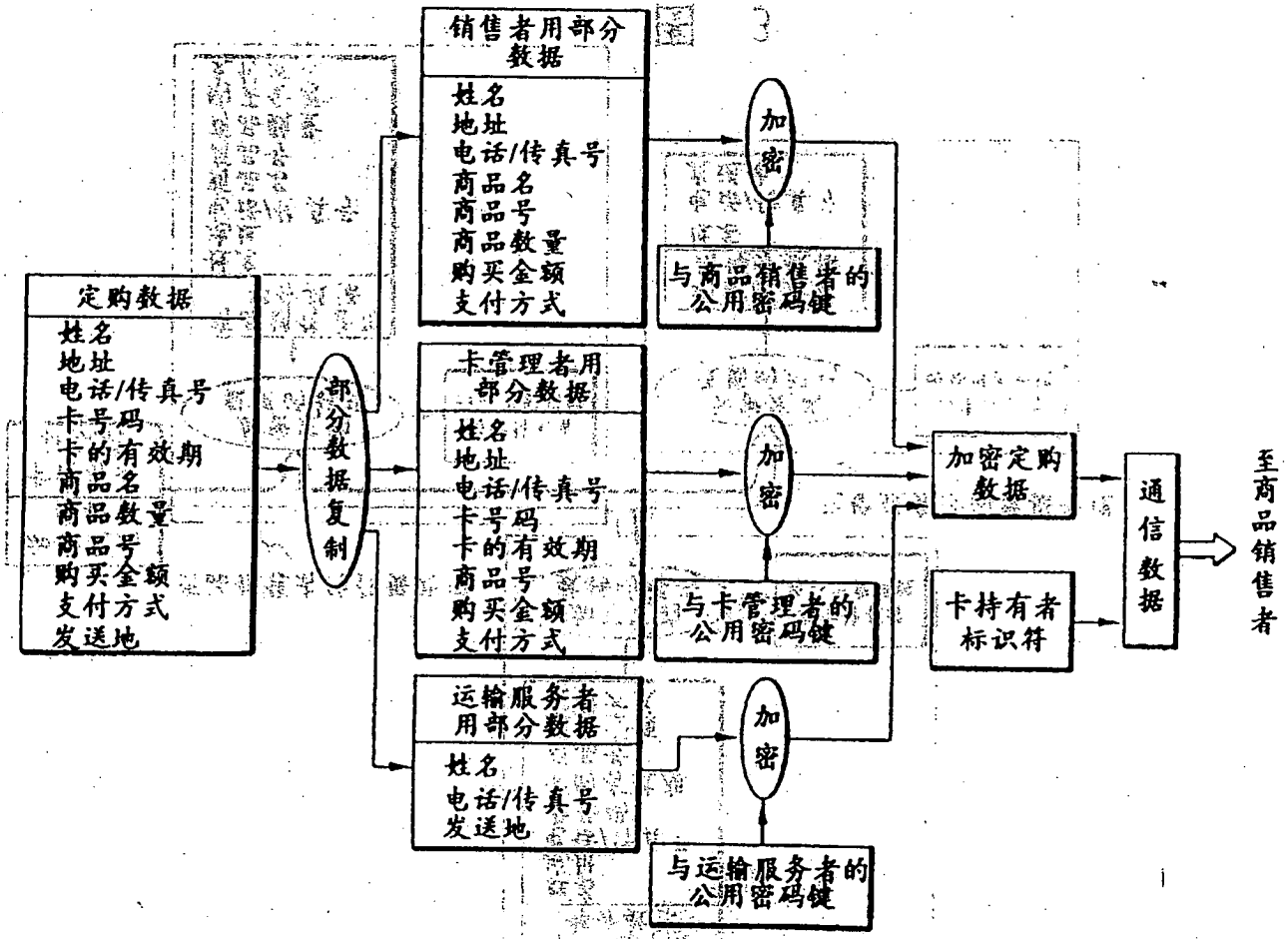

定购数据
姓名
地址
电话/传真号
卡号码
卡的有效期
商品名
商品数量
商品号
购买金额
支付方式
发送地
部分数据复制
销售者用部分数据
姓名
地址
电话/传真号
商品名
商品号
商品数量
购买金额
支付方式
卡管理者用部分数据
姓名
地址
电话/传真号
卡号码
卡的有效期
商品号
购买金额
支付方式
运输服务者用部分数据
姓名
电话/传真号
发送地
加密
加密
加密
与商品销售者的公用密码键
与卡管理者的公用密码键
与运输服务者的公用密码键
加密定购数据
卡持有者标识符
通信数据
至商品销售者

图 2

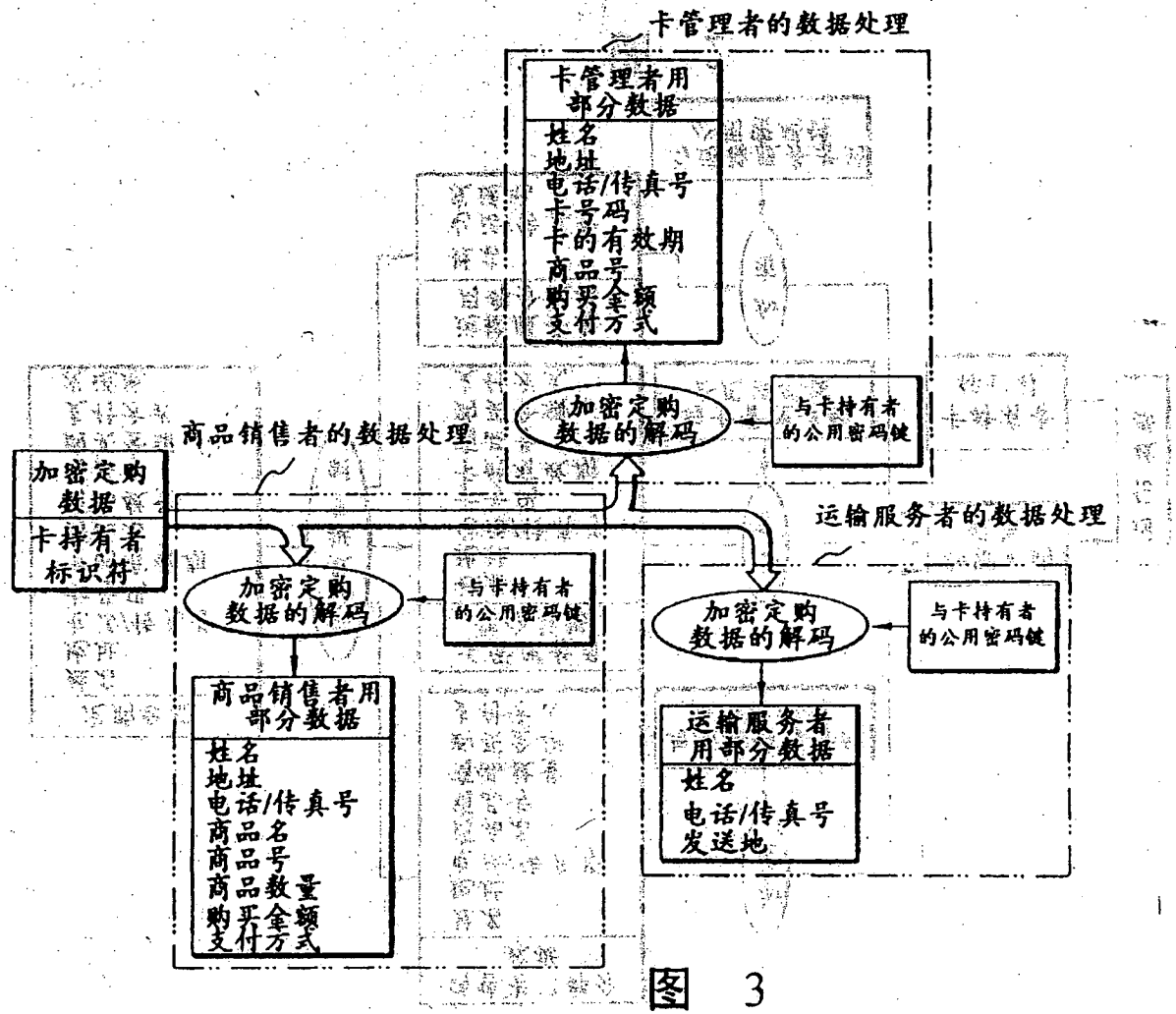

卡管理者的数据处理
卡管理者用部分数据
姓名
地址
电话/传真号
卡号码
卡的有效期
商品号
金额
支付方式
加密定购数据的解码
与卡持有者的公用密码键
商品销售者的数据处理
加密定购数据
卡持有者标识符
加密定购数据的解码
与卡持有者的公用密码键
商品销售者用部分数据
姓名
地址
电话/传真号
商品名
商品号
商品数量
购买金额
支付方式
运输服务者的数据处理
加密定购数据的解码
与卡持有者的公用密码键
运输服务者用部分数据
姓名
电话/传真号
发送地

图 3